Abstract

Method for secure data transmission

The invention relates to a method for secure data transmission, particularly between a tachograph (51) in a commercial vehicle and memory cards (50), where a first subscriber (T1) has a memory (6, 22) with entries (31-35) comprising identifiers (4) and security certificates (Cert) from second subscribers (T2). Methods for secure data transmission are becoming increasingly important and are frequently associated with a high level of computation complexity. For this reason, the object of the invention is to reduce the computation time for this without security losses. It is proposed that the first subscriber (T1) fetch an identifier (4) from the second subscriber (T2) and compare it with stored identifiers (4). If the identifier (4) matches, a security certificate (Cert) associated with this identifier (4) is the basis for a subsequent data transmission, and if the identifier (4) does not match then security certificate verification is performed.

(Figure 1)